

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

ROBERT V. TOWNES, IV, )  
Individually and on behalf of all )  
Persons similarly situated, )  
                                )  
                                Plaintiff, )  
                                )  
                                )  
v.                            ) C.A. No.: 04-1488-JJF  
                                )  
                                )  
TRANS UNION, LLC and )  
TRUELINK, INC., )  
                                )  
                                Defendant, )

**OBJECTIONS OF STEVEN AND MELODY  
MILLETT TO PROPOSED CLASS ACTION SETTLEMENT**

Christopher J. Curtin  
ERISMAN & CURTIN  
DE Bar Id. No. 0226  
Erisman & Curtin  
629 Mount Lebanon road  
Wilmington, Delaware 19803  
Phone: (302) 478-5577  
Facsimile: (302) 478-5494  
Email: [ccurtin659@aol.com](mailto:ccurtin659@aol.com)

COUNSEL FOR STEVEN G. MILLETT  
AND MELODY J. MILLETT

FILED: August 20, 2007

Steven Millett and Melody Millett ("the Milletts") hereby object to the proposed settlement ("Settlement Agreement") that has been preliminarily approved by this Court in the case of Robert V. Townes, IV v. Trans Union, et al., Case No. 04-1488-JJF, District of Delaware ("Townes Action"). (D.I. 66).<sup>1</sup> The Milletts reside at 12449 Slater Street, Overland Park, Kansas 66213, and their telephone number is 913-685-5826.

The Milletts are named plaintiffs in a separate class action, Millett v. Truelink, Inc., Case No. 05-599-SLR, District of Delaware ("Millett Action"). The Millett Action involves the Credit Monitoring service sold by TrueLink, Inc. ("TrueLink"). The Milletts purchased Credit Monitoring from TrueLink on various dates from 2003 through 2005. The Credit Monitoring service is one of the services that is the subject of the Townes Action. TrueLink is a defendant in the Townes Action. The Milletts are filing these objections in order to protect their interests, and the interests of the class of persons whom they represent in the Millett Action, in relation to the Credit Monitoring service.

The Milletts intend to appear at the fairness hearing through their counsel, Christopher J. Curtin, Michael W. Blanton and Barry R. Grissom. In addition, Melody Millett intends to appear at the fairness hearing in person. Steven Millett does not intend to appear at the fairness hearing in person. The Milletts do not intend to call any persons

---

<sup>1</sup>

These objections refer to documents that have been filed in two separate actions: Robert V. Townes, IV v. Trans Union, et al., Case No. 04-1488-JJF, District of Delaware ("Townes Action") and Millett v. Truelink, Inc., Case No. 05-599-SLR, District of Delaware ("Millett Action"). Pursuant to local rules, Plaintiffs will reference these documents by docket number. However, it should be noted that these docket numbers are associated with two different cases.

to testify in support of their objections other than their counsel. The Milletts have not appeared as settlement objectors in any other class action during the past five years. The Milletts' counsel have not appeared as counsel for settlement objectors in any other class action during the past five years. The Milletts have previously filed a motion to intervene in Browning v. Yahoo! Inc., et al., Case No. C04-01463, Northern District of California, San Jose Division.

The Milletts believe that the interests of the class of persons for whom they seek certification in the Millett Action will be substantially impaired by the Settlement Agreement for which this Court has granted preliminary approval. The Settlement Agreement defines the scope of the release in an unreasonably broad manner that encompasses the completely separate claims of the class that is represented in the Millett Action. The Milletts are concerned that the over broad Settlement Agreement will have the effect of permanently eliminating the claims of the Millett class without providing the Millett class with any relief that relates to the specific claims that are at issue in the Millett class action. In short, the Milletts are concerned that the Settlement Agreement, due to its overly broad language, might have the effect of barring a class of claimants from pursuing their claims in litigation, while affording that class no effective relief under the Settlement Agreement.

## **GROUND FOR OBJECTIONS**

### **I. THE CREDIT MONITORING SERVICE CONSISTS OF TWO PRIMARY COMPONENTS: CREDIT REPAIR SERVICES AND IDENTITY THEFT PROTECTION SERVICES.**

The Credit Monitoring service consists of two primary components: credit repair services and identity theft protection services. The Townes Action focuses on credit repair services. The Millett Action focuses on identity theft protection services. The Settlement Agreement in the Townes Action provides relief in relation to the component of the Credit Monitoring service that relates to credit repair services and provides essentially no relief that is geared to the identity theft protection component of Credit Monitoring.

#### **A. The Townes Complaint.**

The Complaint in the Townes Action (“Townes Complaint”) states claims related to credit repair services. (D.I. 1). The Townes Complaint alleges that each of the Defendants are “credit repair organizations.” (D.I. 1, ¶ 1). The Townes Complaint alleges that Defendants “operate in violation of the consumer protection provisions of the federal Credit Repair Organizations Act (‘CROA’).” (D.I. 1, ¶ 1).

The Plaintiff in the Townes Action purchased services from Defendants “in order to improve his credit record, credit history, and credit rating.” (D.I. 1, ¶ 4). The services that Plaintiff purchased from Defendants “included identification of specific factors to help the consumer obtain favorable consideration by lenders in evaluating the capacity

and creditworthiness of the consumer [and] summaries and explanations of debt and credit scores to enable the consumer to improve his or her score over time.” (D.I. 1, ¶ 8).

The Townes Complaint focuses almost exclusively upon alleged violations of the CROA. (D.I. 1, ¶¶ 1, 10-12, 14-18, 21 and 25-27).<sup>2</sup> The Townes Complaint does not contain any references to any services that pertain to protecting consumers from identity theft.

In short, the Townes Complaint focuses solely upon representations that were made and actions that were taken with regard to the provision of credit repair services. The services at issue in the Townes Complaint are services offered to improve a person’s credit record, credit history, and credit rating. The Townes Complaint alleges that Defendants’ conduct violates the CROA. The Townes Complaint does not address any services that are intended to provide protection from identity theft, nor state any claims that pertain to the provision of such services.

#### **B. The Millett Complaint.**

The Fourth Amended Complaint in the Millett Action (“Millett Complaint”) states claims relating to services that purport to protect consumers against identity theft. (D.I. 76). The Millett Complaint alleges that Truelink sold identity theft protection services

---

<sup>2</sup>

The Townes Complaint contains a brief count stating a claim of unjust enrichment. (D.I. 1, ¶¶ 28-30). However, this count merely seeks reimbursement of the money that was received through the conduct that constituted violations of the CROA. Furthermore, the Prayer for Relief speaks solely in terms of relief under the CROA.

under the names Credit Monitoring or Online Credit Monitoring (“Credit Monitoring”). (D.I. 76, ¶ 8). More specifically, the Millett Complaint alleges that Truelink marketed its services as “[p]rotecting members against identity theft and fraud” and “[a]llowing members to immediately find out about fraudulent activity.” (D.I. 76, ¶ 10). The Millett Complaint also alleges that Truelink incorporated these same promises into the contract by which it sold Credit Monitoring. (D.I. 76, ¶ 16).

Count I of the Millett Complaint alleges that Truelink has violated the Kansas Consumer Protection Act in that Truelink has promised to provide identity theft protection services but Truelink has failed to provide the services that were promised or has provided services that were different in content and quality from the services that were promised. (D.I. 76, ¶¶ 33-47). Count II of the Millett Complaint alleges that Truelink has breached its promise to provide identity theft protection services in that Truelink has failed to provide the services that were promised. (D.I. 76, ¶¶ 48-53).<sup>3</sup>

In short, the Millett Complaint focuses solely upon representations that were made and actions that were taken with regard to the provision of **identity theft protection services**. The services at issue in the Millett Complaint are services that are offered to protect consumers from identity theft and credit fraud. The Millett Complaint alleges that Truelink’s conduct violates the Kansas Consumer Protection Act and constitutes a breach

---

<sup>3</sup>

The Millett Complaint originally contained counts stating claims for violations of the CROA and the Credit Reporting Agencies Act. However, these counts were voluntarily dismissed by the Milletts on March 5, 2007 because the Milletts did not want to encroach upon the CROA claims being pursued in the Townes Action. (D.I. 98, ¶ 6).

of contract. These allegations specifically pertain to the provision of **identity theft protection services.**

**C. The Two Components Of Credit Monitoring – Credit Repair Services And Identity Theft Protection Services – Are Substantially Different.**

As noted above, the credit repair services that are provided as part of Credit Monitoring are intended to help a consumer obtain favorable treatment from creditors by improving his credit score. Credit Monitoring purports to help a consumer improve his credit score by helping him to identify specific factors that can be addressed in order to improve his credit score. For example, Credit Monitoring purports to provide summaries and explanations of debt and credit scores to enable a consumer to improve his credit score over time.

The identity theft protection component of Credit Monitoring serves a completely different purpose and accomplishes that purpose by different means. The identity theft protection component of Credit Monitoring serves to protect consumers against identity theft and fraud. Credit Monitoring purports to accomplish this purpose by providing a consumer with a warning if the consumer has become a victim of identity theft and fraud.

As explained below, Credit Monitoring cannot actually provide the promised identity theft protection services.

**II. THE IDENTITY THEFT PROTECTION COMPONENT OF CREDIT  
MONITORING CANNOT WORK AS PROMISED.**

The identity theft protection component of the Credit Monitoring service cannot provide the broad protection that is promised in the marketing materials and contracts that are used to sell Credit Monitoring. The reasons for this failure are spelled out in some detail below. The Milletts have retained experts to analyze the Credit Monitoring service and the marketing materials that are used to market Credit Monitoring. The explanation set forth below includes reference to those expert analyses.

The following explanation of the deficiencies of the identity theft protection component of the Credit Monitoring service are set forth so that this Court may understand the serious deficiencies in the Credit Monitoring service. It is important to note that the deficiencies of the Credit Monitoring service discussed below are not addressed in the Settlement Agreement that is before this Court. As noted previously, the Settlement Agreement only addresses the credit repair component of Credit Monitoring, not the identity theft protection component.

**A. The Nature Of Identity Theft.**

Identity theft is commonly defined as the use of some item of a person's personal information, without that person's permission, for purposes of committing fraud or theft. (Expert Report of Robert Ellis Smith, p. 6, attached hereto as Exhibit E). Most consumers consider the misappropriation of a single personal identifier to constitute identity theft. For example, a survey conducted by one the Milletts' experts establishes

that 99% of survey participants agree that someone using a consumer's Social Security number with a different name and address to obtain credit or employment constitutes identity theft. (Expert Report of Ronald L. Dimbert, pp. 2, 9, attached hereto as Exhibit F). Identity theft is not limited solely to the fraudulent use of information for credit purposes. (Exhibit E, p. 7).

#### **B. The Credit Reporting Process.**

Credit Reporting Agencies ("CRAs") compile consumer information, such as payment history, which is submitted by creditors and other businesses, and disseminate compilations of that information to creditors, insurance companies, employers, and others with a legitimate business need for that information. (FTC Report, p. 1, attached hereto as Exhibit H). Each record is attached to identifying information such as name, Social Security number, address and birth date. (Exhibit H, p. 9). The CRAs organize these records into files, which refer to all records that the CRA believes to belong to the same person. (Exhibit H, p. 9).

The process by which the CRAs collect and match consumer information (i.e. compile credit files) can be summarized as follows:

- (1) Consumer information is supplied to a furnisher (creditor or other entity that intakes consumer information);
- (2) The furnisher submits consumer information to the CRAs (may be submitted to one or more CRAs);

(3) The CRA attempts to match the consumer information to its consumer files; and

(4) The CRA updates its consumer files with the new information.

(Exhibit H, p. 9). The matching process in step three is fraught with difficulties and information is not always matched with the correct consumer. (Exhibit H, pp. 13-14, 36-46). The CRAs use an algorithm in an attempt to match incoming data with existing consumer files. (Exhibit H, p. 45). If a match is made, then the information is associated with a particular consumer file. (Exhibit H, p. 45). If no match is made, then a new file is created. (Exhibit H, p. 45). Once additional data is obtained in the future, the new file may be merged into an existing file or it may be maintained as a new file. (Exhibit H, p. 45).

A consumer file contains the following information: (1) information to identify the consumer; (2) credit account information; (3) public records; (4) collection accounts; and (5) inquiries wherein a subscriber requests a report. (Exhibit H, pp. 10-11).

One service that the CRAs provide is the ability to monitor consumer files for specific types of activity. TransUnion calls this service a “Watch.” (Deposition of Kate Anderson, Exhibit C, p. 58). When an entity uses this service, it requests that TransUnion set a Watch for a specific consumer file and TransUnion thereafter provides that entity with alerts when certain activity occurs in that file. (Exhibit C, p. 58).

**C. TrueLink's Credit Monitoring Service.**

TrueLink first offered its Credit Monitoring service for sale on or about July 29, 2001. (Responses to Plaintiffs' First Interrogatories in the Millett Action, No. 3, attached hereto as Exhibit I). Credit Monitoring is available on a web portal called TrueCredit. Credit Monitoring purports to guard against identity theft by notifying a consumer of critical changes to his or her credit report. (Deposition of Lucy Duni, p. 108, attached hereto as Exhibit J).

The Credit Monitoring service notifies a consumer when certain critical changes occur in the consumer's credit report. TrueLink is notified by the CRA that a change has taken place in a consumer's credit report. (Exhibit B, p. 26). TrueLink then sends the consumer an email advising him or her that there has been a change to the credit report that should be reviewed by the consumer. (Exhibit B, p. 26; Exhibit C, p. 15). This notice is commonly referred to as a "credit alert." (Exhibit C, p. 15).

The Credit Monitoring service is essentially a conduit through which information from TransUnion is passed to a consumer. (Exhibit J, pp. 109, 112). When a consumer enrolls in Credit Monitoring, TrueLink places a request with TransUnion that a Watch be set for that consumer. (Exhibit C, p. 58, 175-81). TrueLink then receives alerts for that consumer from TransUnion if the Watch is set to trigger such an alert for that consumer. (Exhibit C, p. 58).

TransUnion monitors a consumer's credit file for specific and limited critical changes. The critical changes that Credit Monitoring alerts consumers about are the items a TransUnion Watch monitors. (Exhibit J, p. 108). TransUnion determines the

triggers for a Watch and furnishes the credit alerts; it determines when a transaction qualifies as a credit alert. (Exhibit C, p. 21). Because TrueLink merely passes on Watch information from TransUnion, TrueLink is unable to increase the number of items monitored by TransUnion. (Exhibit J, pp. 108-109). TrueLink takes the information provided by TransUnion, reformats it, and passes it on to the consumer. (Exhibit C, pp. 44-45).

Credit Monitoring does not inform a consumer about all changes to a credit report. (Deposition of Brian Matis, p. 32, attached hereto as Exhibit A). Credit Monitoring only informs the consumer about changes in the specific items TransUnion determines it will monitor. (Exhibit A, p. 32). Furthermore, a consumer who learns of identity theft through Credit Monitoring only learns of the theft after it occurs because TrueLink can only send an alert after the triggering event occurs. (Exhibit C, p. 102). Credit Monitoring does not notify the consumer about all types of identity theft. For example, Credit Monitoring will not inform a consumer if an identity thief is using the consumer's Social Security number, but no other personal identifiers. (Exhibit C, p. 135). Similarly, if someone is using the consumer's Social Security number for a non-credit purpose, the consumer would not be notified. (Exhibit B, p. 118).

#### **D. Problems With TrueLink's Credit Monitoring Service.**

As discussed above, Credit Monitoring merely passes information to the consumer that TrueLink has obtained from TransUnion. Thus, the accuracy and completeness of the information and monitoring that TrueLink provides to consumers is

limited by the accuracy and completeness of the information that is maintained by TransUnion.

As explained more fully below, the Credit Monitoring service cannot provide accurate and complete information because it relies upon a credit report as its sole source of information and a credit report is not a good tool for identity-theft protection. A credit report does not provide all of the information that a person would need to detect all forms of identity theft. (Response to Plaintiffs' First Request for Admission to Defendant TrueLink, Inc. in the Millett Action, No. 35, attached hereto as Exhibit D). In a variety of scenarios – some of which are identified below – a CRA may not have information relevant to the theft of a consumer's identity. Thus, Credit Monitoring cannot notify consumers of all incidents of identity theft or all information that would be useful in protecting against identity theft.

The underlying reasons for the failure of the Credit Monitoring service can be divided into two broad categories: (1) problems arising from incomplete information in the credit report, and (2) problems arising from the failure to properly match data with the correct consumer.

#### **1. Problems arising from incomplete information in the consumer's credit report.**

Many types of transactions are either not reported to CRAs or are not regularly reported to CRAs. (Exhibit C, p. 118). Some examples of such transactions are as follows:

- If a person provides another person's Social Security number to law enforcement personnel, that misuse of the Social Security number would not appear on the credit report. (Exhibit A, p. 24).
- If a person used another person's Social Security number to obtain a driver's license, that misuse of the Social Security number would not appear on the credit report. (Exhibit A, p. 24).
- Rental information is generally not reported to the CRAs. (Exhibit H, pp. 78, 80).
- Accounts with utilities generally are not reported to the CRAs. (Exhibit C, p. 118; Exhibit H, p. 81). In fact, utilities may be barred by regulation from providing such information to the CRAs. (Exhibit H, p. 81).

In short, a great deal of information regarding identity theft is never reported to CRAs and is never included in a credit report. As a result, this information would never trigger an alert under the Credit Monitoring service.

Even for those types of information that are commonly reported to the CRAs, the reporting is incomplete. Some creditors do not furnish information to the CRAs at all, and some report to only one or two of the CRAs. (Exhibit H, p. 12). In addition, a creditor may deliberately withhold information for strategic reasons. (Exhibit H, p. 12). For instance, some lenders, particularly subprime lenders, choose to withhold positive credit information about their consumers to prevent their most profitable consumers from receiving competing offers. (Exhibit H, p. 12). Thus, even types of information that

would commonly appear in a credit report may not appear in a particular consumer's credit report due to incomplete reporting.

Due to problems with the incompleteness of information in the consumer's credit report, a consumer can be a victim of identity theft and evidence of that theft will never appear in the credit report. This is true even for classic incidents of credit identity theft such as when an identity thief opens a new credit card using a consumer's personal identifying information. For example, if an identity thief opens a new credit account and the creditor fails to report that new account to the CRAs (or to the particular CRA that is being used for the Credit Monitoring service), then the consumer will not be notified of that new account and will not be notified that he or she has become a victim of identity theft.

**2. Problems arising from the failure to properly match data with the correct consumer.**

Even if a creditor does report account information to the CRAs, this information may not be properly matched with the consumer in question.

A CRA may have problems assigning data to the proper consumer files. (Exhibit H, p. 13). When a CRA's system fails to correctly assign a consumer's data, it can create either a "mixed file" or a "fragmented file." (Exhibit H, p. 13). A "mixed file" refers to a file containing information pertaining to more than one consumer. (Exhibit H, p. 13). A "fragmented file" refers to a situation where more than one file in a CRA database exists for the same consumer. (Exhibit H, p. 13).

Problems with matching may be caused by either the consumer or the furnisher that records and reports the consumer's information. (Exhibit H, p. 41). Problems with the information the consumer provides can arise either from error or deliberate choice (such as identity theft). (Exhibit H, p. 41). Having collected information from a consumer, a creditor also may make mistakes when entering the consumer's data into its system. (Exhibit H, p. 41).

When a CRA cannot match new account information with a specific consumer, it creates a new file to store that information. (Exhibit H, p. 45). As the CRA receives additional information in relation to that account, it may be able to match the file to a specific consumer at a later time, in which case the new file will be merged into an existing consumer's credit file. (Exhibit H, p. 45). Otherwise, the new file will be maintained as a separate file. (Exhibit H, p. 45).

Due to these and other matching failures, a consumer may be a victim of identity theft but not have any evidence of that identity theft appear in his or her credit report. For example, if an identity thief opens a credit account using a consumer's personal identifying information, and that account is reported to TransUnion without the consumer's Social Security number being identified, TransUnion might be unable to ascertain which credit file is the appropriate file for the inaccurate or partially complete information. Thus, TransUnion will create a second file and place the information pertaining to the new credit card there instead. If a Watch is set for that consumer, the Watch would not detect this new account because the account would not be associated

with the consumer's credit report. Thus, the Credit Monitoring service would not alert the consumer of this new account even though it is a clear instance of identity theft.

There is no doubt that matching failures occur. (Exhibit H, pp. 13, 41, 45). It is equally clear that such errors are common. A 2000 Consumers Union study reported that more than half of consumer credit reports contain errors. (Exhibit H, p. 23). A June 2004 U.S. Public Interest Research Group study reported that one in four of the consumer reports surveyed contained serious errors. (Exhibit H, p. 23). In total, nearly eight out of ten (79%) of the consumer reports surveyed reportedly contained some error. (Exhibit H, p. 24).

There is also no doubt that TrueLink was aware of the problems regarding matching consumer credit reports. In 2005, TrueLink identified a need to improve consumer record matching because it was getting too many "no-hits" from the CRA. This occurred when the CRA was unable to provide a matching credit file for the consumer who was attempting to enroll. (Exhibit C, p. 52). In other words, the CRA data was so faulty that the CRA could not match a potential purchaser of Credit Monitoring to a particular credit file in the first instance.

#### **E. Marketing Of Credit Monitoring.**

Despite the inability of the Credit Monitoring service to detect a wide spectrum of identity-theft incidents, TrueLink marketed the Credit Monitoring service as providing very broad protection against identity theft. In fact, TrueLink marketed the Credit

Monitoring service as providing "complete identity theft protection." (Marketing Materials, pp. 7-8, attached hereto as Exhibit G).

The marketing materials for Credit Monitoring include numerous other representations regarding the broad protection provided by Credit Monitoring. The following are examples:

- "You'll always be up-to-date about credit report changes and early warning signs of identity fraud." (Exhibit G, pp. 3-5).
- "With Credit Monitoring you'll be up-to-date with your credit, informed about any fraudulent activity, and certain about your credit standing." (Exhibit G, p. 6).
- "You can secure your credit, your identity, & your peace of mind for just \$9.95/year with the Web's most affordable credit monitoring service – weekly Credit Alerts." (Exhibit G, p. 1). "Stay informed about your credit and your identity – without even lifting a finger." (Exhibit G, p. 1).
- "You can secure your credit, your identity, & your peace of mind for just 12 cents a day with TrueCredit's award-winning Credit Monitoring services." (Exhibit G, p. 9).
- "You have anti-theft & protection devices for your home ... and your car ...

But what about your identity?

Now you can secure your credit, your identity, & your peace of mind for less than 3 cents a day." (Exhibit G, p. 2).

These marketing materials generally indicate that the purchaser of Credit Monitoring will be warned about "identity fraud" and "fraudulent activity." These marketing materials also distinguish between your "credit" and your "identity," indicating that both will be protected by Credit Monitoring. The last of the above-referenced items goes so far as to compare Credit Monitoring to a general purpose alarm system, implying that Credit Monitoring will act as a general purpose alarm system for identity theft.

The marketing materials for Credit Monitoring produce extremely high expectations among consumers. The Milletts have had a survey conducted by a marketing expert. This marketing expert was retained by the Milletts to conduct research to understand consumer expectations that resulted from viewing an advertisement for the Credit Monitoring service. (Exhibit F, p. 1). Consumers were shown an advertisement for Credit Monitoring and were asked about their expectations in relation to the Credit Monitoring service. (Exhibit F, p. 1). The results were as follows:

- 95% expected to receive notice if another person is using any of his or her personal information without his or her permission, and only 1% did not expect such notice. (Exhibit F, p. 10).
- 94% expected immediate notification of credit report changes, and only 1% did not expect such notification. (Exhibit F, p. 10).
- 90% expected a credit report containing all information necessary to protect him or her against fraudulent activity, and only 3% did not expect such a report. (Exhibit F, p. 10).

- 83% expected complete identity-theft protection, and only 2% did not expect such protection. (Exhibit F, p. 10).
- 98% expected notice if someone was taking action that impacts his or her credit, and only 1% did not expect such notice. (Exhibit F, p. 11).
- 93% expected notice if someone was using his or her identity in a manner that would result in him or her needing to seek legal help, and only 3% did not expect such notice. (Exhibit F, p. 11).
- 86% expected notice of someone using his or her Social Security number, and only 3% did not expect such notice. (Exhibit F, p. 11).
- 78% expected notice of someone using his or her identity to obtain a driver's license, and only 5% did not expect such notice. (Exhibit F, p. 11).

In short, the marketing materials for Credit Monitoring lead consumers to expect that the service will provide notice of incidents of identity theft that the service cannot possibly provide.

Even TrueLink's own employee acknowledged that Credit Monitoring cannot provide the promised level of protection. Brian Matis, a product developer for TrueLink, testified that Credit Monitoring cannot completely protect a consumer from identity theft. (Exhibit A, p. 80). In fact, when Mr. Matis was asked during the course of his deposition whether a consumer could completely protect him or herself from identity theft, he stated: "That sounds to me like completely protecting yourself from a car accident, and there's – there's no conceivable way." (Exhibit A, p. 79).

**III. THE TOWNES SETTLEMENT DOES NOT PROVIDE ANY RELIEF  
RELATING TO THE DEFICIENCIES IN THE IDENTITY THEFT  
PROTECTION COMPONENT OF THE CREDIT MONITORING  
SERVICE AND THE MISREPRESENTATIONS REGARDING THAT  
COMPONENT OF THE CREDIT MONITORING SERVICE.**

As explained above, the identity theft protection services that are addressed in the Millett Action are substantially different from the credit repair services that are addressed in the Townes Action. Furthermore, the Milletts have gathered substantial evidence establishing that the identity theft protection component of the Credit Monitoring service cannot work as advertised, and establishing that the marketing materials used to sell Credit Monitoring are seriously misleading in terms of the claims that are made in relation to identity theft protection services. As explained below, these two facts warrant rejection of the Settlement Agreement because the Settlement Agreement is so broad that it may release claims pertaining to the identity theft protection component of the Credit Monitoring service without providing any relief in relation to those claims.

**A. The Release Provision Of The Settlement Agreement Is Over broad  
And May Impair The Separate Class Claims Being Pursued In The  
Millett Action.**

As noted previously, the claims addressed in the Townes Action and the Millett Action are substantially different. The Townes Action focuses upon credit repair services that are offered as part of the Credit Monitoring service. The Millett Action focuses upon

identity theft protection services that are offered as part of the Credit Monitoring service. Thus, while both actions deal with the Credit Monitoring service, the actions address totally different aspects of the Credit Monitoring service.

The distinction between the various services that are offered as part of the Credit Monitoring service is crucial. This distinction may be better illustrated by way of an analogy. For example, an automobile manufacturer may manufacture and market a particular vehicle and that vehicle may be the subject of two different lawsuits. One lawsuit may argue that the vehicle is defective because the steering mechanism does not work properly and the other lawsuit may argue that the vehicle is defective because the brakes do not work properly. Although both claims pertain to the same vehicle, and both claims allege a defect in the vehicle, the claims are clearly distinct and the interests of the persons bringing those claims are similarly distinct. In this case, the claims and interests involved in the Millett Action and the Townes Action are likewise distinct.

Unfortunately, although the claims and interests that are at issue in the Millett Action and the Townes Action are distinct, the parties in the Townes Action have now entered into a Settlement Agreement that attempts to dispose of the totally separate claims that are at issue in the Millett Action.

The Settlement Agreement includes a very broad release provision. The exceptional breadth of the release provision is exhibited by the definition of Released Claims which states in pertinent part as follows:

“Released Claims” means any and all claims, actions, demands, causes of action, suits, obligations, damages, rights or liabilities, of any nature and description whatsoever, known or unknown, present or future, concealed

or hidden, liquidated or unliquidated, fixed or contingent, anticipated or unanticipated, whether statutory, in tort, contract, law, equity or others, that have been, could have been or might in the future be asserted by Plaintiff in the Townes Action or the Settlement Class members or any of their respective heirs, spouses, executors, administrators, partners, attorneys, predecessors, successors, assigns, agents and/or representatives, and/or anyone acting or purporting to act on their behalf, arising out of the offering, marketing, sale, purchase, delivery, or use of, or representations and advertisements concerning, the Offerings.

(D.I. 66, ¶ 2.20). Pursuant to this definition of Released Claims, the Settlement Agreement would release all claims of any type pertaining to Credit Monitoring, regardless of whether those claims had anything to do with credit repair services. This definition is so broad that it would incorporate many persons who do not fall within the class identified in the Townes Complaint. More to the point, this definition would include persons who fall within the class identified in the Millett Complaint.

To refer back to the analogy of the claims for a defective vehicle, it is as if a settlement agreement had been entered in the action involving allegations of defective brakes, and the settlement agreement also disposed of claims pertaining to defective steering mechanism even though the settlement provided absolutely no relief to persons who had a defective steering column.

**B. The Settlement Agreement Does Not Provide Relief That Addresses The Separate Claims Being Pursued In The Millett Class Action.**

The Settlement Agreement provides that, in exchange for the release from future liability, Defendants agree to make changes to their contracts and marketing materials.

(D.I. 66, ¶¶ 5.1.1 - 5.1.6). With one limited exception, all of these changes pertain to

credit repair services. (D.I. 66, ¶¶ 5.1.1 - 5.1.5). The exception is a section which provides that Defendants will provide the following disclaimer on their websites:

A disclaimer explaining that Defendants' credit monitoring Offerings monitor only the credit file associated with the purchasing consumer, and do not monitor, compare or cross-reference the credit file associated with the purchasing consumer to any other credit file(s) maintained by the applicable credit bureau(s).

(D.I. 66, ¶ 5.1.6). None of the proposed changes involve contract or marketing language that specifically involves identity theft protection services. (D.I. 66, ¶¶ 5.1.1 - 5.1.6). These changes to contract and marketing language are referred to collectively in the Settlement Agreement as "Injunctive Relief." (D.I. 66, p. 21).

The Settlement Agreement also provides for in-kind relief ("In-Kind Relief") as follows: "Defendants, through TrueLink, will provide three (3) months of Trans Union Credit Monitoring, as it is offered by TrueLink as of March 1, 2007, (the "In-Kind Relief") to each Class member who purchased any Offering from Defendants."

Neither the Injunctive Relief nor the In-Kind Relief provide any relief that is meaningful in terms of the separate claims that are being pursued in the Millett Action. Specifically, the Injunctive Relief and the In-Kind Relief do not address injuries that arose from the Defendants' failure to provide adequate identity theft protection services and Defendants' misrepresentations regarding the identity theft protection services that were provided.

The Injunctive Relief is geared almost solely to claims pertaining to credit repair services. The In-Kind Relief is even worse — Defendants propose to give class members

three free months of the very service that the Millett Action claims does not work in the first place.

In short, the problem with the Settlement Agreement is that it purports to settle claims that are not the subject of the underlying complaint. Furthermore, the relief granted under the Settlement Agreement would be of no benefit to persons bringing different types of claims, such as the putative class in the Millett Action. For these reasons, the Settlement Agreement may have the effect of releasing valid and significant claims of class members without providing any relief that addresses the released claims.

### **CONCLUSION**

For the reasons stated herein, the Milletts respectfully request that this Court deny final approval of the Settlement Agreement proposed in the Townes Action.

Respectfully submitted,

/s/ Christopher J. Curtin  
Christopher J. Curtin  
DE Bar Id. No. 0226  
Erisman & Curtin  
629 Mount Lebanon road  
Wilmington, Delaware 19803  
Phone: (302) 478-5577  
Facsimile: (302) 478-5494  
Email: ccurtin659@aol.com

/s/ Barry R. Grissom  
Barry R. Grissom, Esq.  
KS Bar. Id. No. 10866  
7270 W. 98th Terrace  
Building 7, Suite 220  
Overland Park, Kansas 66212  
Phone: (913) 341-6616

and

Michael W. Blanton,  
MO Bar. Id. No. 46490  
Swanson Midgley, LLC  
2420 Pershing Road, Ste. 400  
Kansas City, Missouri 64108  
Phone: (816) 842-6100

COUNSEL FOR OBJECTING PARTIES  
STEVEN AND MELODY MILLETT

For the above and foregoing reasons, Steven and Melody Millett, object to the proposed class settlement and pray the Court deny approval of same.

Steven Millett  
Steven Millett  
Melody Millett  
Melody Millett

**CERTIFICATE OF SERVICE**

I, Christopher J. Curtin, Esq., hereby certify that on August 20, 2007, a copy of the foregoing Objections of Steven and Melody Millett to Proposed Class Action Settlement, together with all supporting papers and briefs, was served via first-class mail upon the following:

Michael L. McGlamry  
Wade H. Tomlinson  
Pope, McGlamry, Kilpatrick,  
Morrisson & Norwood, LLP  
3455 Peachtree Road, N.E.  
Suite 925  
Atlanta, Georgia 30326

Carmella P. Keener  
Rosenthal, Monhait & Goddess, P.A.  
919 Market Street  
Suite 1401  
Wilmington, Delaware 19801-1070

William Lafferty  
Morris, Nichols, Arsh & Tunnell LLP  
1201 N. Market Street  
Wilmington, Delaware 19801

Wilson F. Green  
Battle, Fleenor, Green,  
Winn & Clemmer LLP  
505 N. 20<sup>th</sup> Street  
Suite 1150  
Birmingham, Alabama 35203

Michael O'Neil  
Paula D. Friedman  
DLA Piper US LLP  
203 N. LaSalle Street  
Suite 1900  
Chicago, Illinois 60601

ERISMAN & CURTIN

/s/ Christopher J. Curtin  
Christopher J. Curtin  
DE Bar Id. No. 0226  
Eisman & Curtin  
629 Mount Lebanon road  
Wilmington, Delaware 19803  
Phone: (302) 478-5577  
Facsimile: (302) 478-5494  
Email: ccurtin659@aol.com

DATE: August 20, 2007